

**U.S. House of Representatives Homeland Security Committee
Subcommittee on Economic Security,
Infrastructure Protection and Cybersecurity**

“How the U.S. Passport Program Enhances Border Security”

**Testimony of
Frank E. Moss
Deputy Assistant Secretary for Consular Affairs**

June 22, 2005

Chairman Lungren, Ranking Member Sanchez, Distinguished Members of the Subcommittee:

I am pleased to have this opportunity to discuss with you the progress that the Department of State has made in introducing biometric elements to the U.S. passport. This innovation represents a significant enhancement to the security of our borders and international travel. In addition to the inclusion of biometrics in U.S. passports, two other aspects of the Department of State's passport program are critical to enhancing U.S. national security: the adjudication process, and the security features of the passport itself. Taken together, these elements constitute a comprehensive approach to passport security. By making sure that U.S. passports are only issued to American citizens, that they are more difficult to counterfeit and that the bearer of the passport is the same person to whom the passport was issued, the Department of State actively enhances the security of this nation.

Today I would like to describe the many ways that the Department of State demonstrates its commitment to the important responsibility for providing passport services. The U.S. passport is arguably the most valuable identity and citizenship document in the world. We at the Department of State are certainly aware of how sought after this document is, not only by American citizens with legitimate travel plans but by illegal immigrants, as well as terrorists and others who would do this nation harm. As portable proof of identity and nationality, the U.S. passport literally opens doors around the world to American citizens who travel or reside abroad or may require assistance from an American Embassy or Consulate. The U.S. passport is also essential for many American citizens to enter the United States upon returning from international travel.

During the last fiscal year the Department of State processed 8.8 million U.S. passport applications. This set a record, exceeding the total from the previous year by more than one million applications and representing a workload increase of some 22 percent. This year, the Department of State forecast a 9 percent increase in passport demand, but is experiencing a 14 percent rise. As of today, the Department has already processed close to 7 million passport

applications during this fiscal year and we are on track to adjudicate more than 10 million passports by the end of fiscal year 2005.

The Intelligence Reform and Terrorism Prevention Act of 2004 also contains a provision addressing the documentary requirements for travel within the Western Hemisphere, referred to as the Western Hemisphere Travel Initiative (WHTI). The legislation requires that the Secretary of Homeland Security, in consultation with the Secretary of State, develop and implement by January 1, 2008 a plan to require U.S. citizens and non-U.S. citizens currently exempt from presenting a passport for travel within the Western Hemisphere to present a passport or other authorized documentation that denotes identity and citizenship when entering the United States. The Department of State, after analyzing the scope of WHTI and other projected growth in passport demand, expects that applications for passports will total about 12 million in FY-2006, about 14 million in FY-2007 and reach a potentially sustainable annual demand of 17 million by FY-2008.

As the Department of State develops plans to address the increase in demand for U.S. passports resulting from normal growth in international travel and the WHTI, we are dedicated to ensuring that security vulnerabilities are not inadvertently created by our efforts to address the increase in workload. While keeping security imperatives in mind, the Department of State also recognizes its responsibility to adjudicate passport applications in a timely and efficient manner to facilitate the travel of U.S. citizens. The free movement of people and goods is essential to U.S. national security, as is our international engagement through personal, commercial, educational and research activities with other nations. We are actively pursuing initiatives to improve the U.S. passport program designed to support both of these objectives.

Strengthening the Adjudicatory Process

A key objective of the Department of State's Office of Passport Services in the Bureau of Consular Affairs is to ensure that U.S. passports are issued only to persons who are legitimately entitled to them. This is particularly important in an era when terrorists, transnational criminals and others seeking to enter the U.S. illegally view travel documents as valuable tools, and when improvements to the physical security of the U.S. passport, such as the use of a digital photograph of the bearer, make it increasingly difficult to counterfeit.

One of the most effective ways to ensure that only those entitled to U.S. citizenship receive a passport is increased information sharing, both within the United States Government and beyond. The Department of State has actively worked to establish data exchange programs with other agencies in a manner that is mutually beneficial and that will keep U.S. passports out of the hands of those who are not eligible to receive them. For example, the Department has a partnership with the Department of Health and Human Services (HHS) that ensures that parents with child support arrearages, who are ineligible to receive passports, do not receive them. The incorporation of over 3 million names in the HHS database into the Department's passport lookout system has also resulted in the recovery of more than \$50 million in delinquent child support.

In April 2004, the Department signed a memorandum of understanding with the Social Security Administration (SSA) that would permit the Department to verify the SSNs of U.S. passport applicants with information in SSA's SSN database. This measure provides another verification tool for passport specialists and consular officials adjudicating passport applications by allowing them to correlate the data provided by a passport applicant with information in SSA's system and use this information to support decisions about an applicant's identity.

The Department has a long-standing and effective working relationship with federal law enforcement agencies that targets passport applicants of particular concern. Today, we have nearly 50,000 names of fugitives or other individuals of interest to law enforcement in the passport lookout system. Half of these were entered individually as a result of our outreach efforts. The other half of these entries are based on U.S. Marshals Service (USMS) federal fugitive warrants, a process that the Department took the initiative to obtain.

To complement the USMS information, work is well underway to add to the passport lookout system an extract of FBI fugitive warrants from the NCIC Wanted Person File. To encourage information exchange with law enforcement officials at the state and local levels, the Assistant Secretary of State for Consular Affairs wrote to all the states' attorneys general.

In 2004, the Department reached an agreement with INTERPOL to provide the Department's lost and stolen passport database to the U.S. National Central Bureau (NCB). The NCB shares the data with INTERPOL, which in turn makes this information available to all INTERPOL member states. The U.S. lost and stolen passport database currently contains the passport numbers of over 620,000 passports.

The Department's Office of Passport Services is also currently working on an agreement with the Terrorist Screening Center that would provide information on American citizens who are either subject to a federal felony arrest warrant or who are considered persons of concern due to a nexus to terrorism or an ongoing investigation. This datashare program will enable the Terrorist Screening Center to learn of the passport application of an individual of interest and, under appropriate circumstances, take law enforcement action.

In addition, the Department's Bureau of Consular Affairs has implemented a cooperative relationship with the National Counter Terrorism Center (NCTC) to provide that organization with direct online access to the Passport Records Imaging System Management (PRISM). This database includes images of the passport applications for all valid passports. The NCTC utilizes this information as a verification tool to support its terrorist watch list responsibilities.

Another important element in safeguarding the adjudicatory process is maintaining an aggressive fraud prevention program. In that regard, the Department of State has undertaken a comprehensive review of its fraud prevention efforts and implemented a number of initiatives, including organizational improvements, enhanced training, regulatory changes, new tools, and new programmatic activities with domestic and international partners. All senior passport specialists now rotate through the fraud prevention office at domestic passport facilities to give them specialized experience in fraud detection. Regulatory changes have been implemented, for example, to require that both parents consent to the issuance of a passport for a child, and to

require the presence of children under the age of 14 when passport applications are executed on their behalf, in order to combat fraud and international parental child abduction. We are making greater use, with the appropriate respect for privacy concerns, of commercial databases to assure that persons applying for passports are who they claim to be.

The focus on fraud prevention is already paying dividends. Statistics for this fiscal year show an increase in referrals to fraud prevention offices, as well as an increase in the referral of presumptive fraud cases to the Department's Bureau of Diplomatic Security (DS) for further investigation. The Bureau of Consular Affairs enjoys excellent cooperation and support from DS, which has the responsibility for criminal investigations involving passport fraud. The statistics about the efficacy of joint Consular Affairs-Diplomatic Security efforts are compelling: so far in fiscal year 2005, DS opened 2401 passport investigations and made 375 arrests, a significant increase over previous years.

Redesigning the Passport

Efforts to strengthen the adjudication process and augment fraud prevention efforts would be less effective if we did not attend to the other key elements of passport security with equal fervor. Turning to the passport itself, the Department recently completed the first cover-to-cover redesign of the document in more than a decade. The new passport includes a host of new security features, including sophisticated new artwork, adopting printing techniques used in the current generation of U.S. currency, and utilizing a variety of other techniques, many of which are only visible under ultraviolet light.

Our objective in designing the new passport is to raise further the bar against counterfeiting or the fraudulent use of lost or stolen passports. Advances including color shifting ink, microprinting, latent image lettering and a security laminate over the biographic data page that includes optical variations, all serve to deter counterfeiters and forgers. The biographic data page has been relocated from the inside of the front cover to the first inside page for added security. The inventory control number for each book is now the same as the passport number. Imagery on the inside pages of the passport incorporates more colors, stylized depictions of iconic American scenes, and includes famous quotations from American history. The new passport, combined with security enhancements in the adjudication process, helps to ensure that only qualified applicants receive U.S. passports.

I am happy to share with the members of the Subcommittee samples of the new passport.

Beyond the physical content of the book itself, we scrutinize each step in the production and delivery process to eliminate vulnerabilities. In addition to improving the quality of the U.S. passport, the Department of State, building on an already excellent collaboration with the Government Printing Office (GPO), is working to secure further the delivery of blank passport books to domestic passport facilities by engaging armored truck service. This mode of delivery service is used by the Department of Treasury to move currency and other valuable documents around the country.

Biometrics

This next generation of U.S. passport, the e-passport, includes biometric technology that will further support the Department's border security goals. Without question, biometrics will strengthen U.S. border security by ensuring that the person carrying a U.S. passport is the person to whom the Department of State issued that passport.

Consistent with globally interoperable biometric specifications adopted by the International Civil Aviation Organization (ICAO) in May 2003, the United States has adopted the facial image as the first generation of biometric identifiers. The new U.S. passport includes a contactless chip in the rear cover of the passport that will contain the same data as that found on the biographic data page of the passport, including a digital image of the bearer's photograph. This data includes the following information about the bearer: the photograph, the name, the date and place of birth, as well as the passport number and the date of issuance and expiration. Looking to the future, the Department decided to require 64 KB of writeable memory on the contactless chip in the event that we subsequently decide to introduce additional biometrics. Should the United States Government decide to change the biometric requirements, this change will be subject to vetting through the Federal Register process.

On June 15, the Department, partnering with the Department of Homeland Security and in collaboration with Australia and New Zealand, launched an operational field test to measure the overall performance of the e-passport, issuing approximately 250 U.S. e-passports to select airline personnel employed by United Air Lines and who fly from Los Angeles to Australia and New Zealand. The Department of Homeland Security has developed separate lanes and installed e-passport readers to test their efficiency. Later this year we will expand this pilot program to include diplomatic and official passports, with national deployment of the e-passport scheduled for 2006.

The Department of State is well aware of concerns that data written to the contactless chip in the e-passport may be susceptible to unauthorized reading. To help reduce this risk, anti-skimming materials that prevent the chip from being read when the passport book is closed or mostly closed will be placed in the passport.

The Department is also seriously considering the adoption of Basic Access Control (BAC) technology to further strengthen the privacy of the data contained on the chip. ICAO recently identified BAC technology as a "best practice" for passport security. BAC technology will prevent the chip from being read until the passport is opened and its machine-readable zone is read electronically. This will serve to "unlock" the chip and permit the chip and reader to communicate through an encrypted session. We are engaged with technical experts from the private sector and the National Institute of Standards and Technology both to assess the risk of unauthorized reading and to evaluate the efficacy of countermeasures. **The bottom line is that we will not issue biometric passports to the general public until we have successfully addressed these concerns.**

The Department is confident that the new e-passport, including biometrics and other improvements, will take security and travel facilitation to a new level. Naturally, the Department

will test comprehensively the operation and durability of the e-passport and work to resolve any issues as they occur. In fact, the Department of State is engaged in a continuous product improvement effort with regard to the U.S. passport. We will continue to monitor technical developments and help conduct research to ensure that we produce a passport that is highly secure, tamper resistant and globally interoperable.

Mr. Chairman, I am grateful for the opportunity today to share with you the Department of State's comprehensive approach to enhancing U.S. border security by augmenting the security of all aspects of the U.S. passport program. The introduction of biometrics is an important advance in continuing to protect the integrity of the world's most respected travel document. At this time I am happy to answer any questions you, the Ranking Member and the other distinguished members of the Subcommittee might have about the Department's biometric passport program or the other facets of the U.S. passport program that I have discussed.